Proceedings of the International Multiconference on
Computer Science and Information Technology, pp. 477 – 483

ISSN 1896-7094

Modern access control based on eye movement analysis and keystroke dynamics

Adrian Kapczyński[1], Paweł Kasprowski[2], Piotr Kuźniacki[2]

[1]Department of Computer science and Econometrics,
Silesian University of Technology,
44-100 Gliwice, Poland
[2]Institute of Informatics,
Silesian University of Technology,
44-100 Gliwice, Poland
{a.kapczynski,p.kasprowski,p.kuzniacki}@polsl.pl

Abstract. The paper presents key aspects connected with modern access control based on behavioral patterns of human being. Two biometric techniques based on eye movement and keystroke dynamics were presented. Quantitative results obtained during examination of systems based on mentioned behavioral methods are convincing to undertake further research work.

1 Introduction

Dynamic development of Information Technology and increase of meaning of information in running business nowadays generated necessity of usage IT solutions which allow successful achievement of declared goals for each company under circumstances of dynamically changing environment. Applying computers in running business causes improvement of activity of company's information system which results in amendment of decisions making processes through delivering accurate and valuable information at the right time and making possible sharing information resources within company. Information system in order to reach the goals should accomplish important criterion concerning reliability, functionality, performance, efficiency and *security*.

Authentication issues are nowadays of utmost importance, and every security administrator should consider choosing appropriate authentication protocols and authentication methods of users who may have access to sensitive data.

Keeping with the latter group in hand, if it is going about user's authentication, there are three groups of authentication methods [2]: based on knowledge (e.g. passwords), based on possession (e.g. smartcard) and based on being – biometric methods (e.g. fingerprint, iris). The last group, namely biometric authentication methods are most likely to become the most secure among of all the methods ever applied. However, before biometrics will become a needful authentication factor a lot of research work shall be undertaken.

After careful analysis of specialist literature [1, 2, 11] it can be stated that key focus in research in area of biometric methods is set on methods based of anatomy of given part of human body (e.g. iris, retina, fingerprint). It has been found that the other group of biometric methods, based on analysis of characteristics of behavioral patterns, is emerging and requires in-depth analysis.

The key point of this article is to present the current state-of-the-art of research carried out by authors in this domain which enables formulation of fundamental basis for further development.

In the first part of the article the biometrics primer was presented and it the second part two developed methods were characterized and put into examination.

2 Biometrics fundamentals

One of the most dangerous security threats is the impersonation and the security services that encounter this threat are called identification (verification).

During identification identity is assigned to a specific individual (one-to-many comparisons) and verification is designed to verify a identity of given user (one-to-one comparison). The verifier can be identified or verified by what he knows (e.g. password), by what he owns (e.g. token) or by anatomical or behavioral characteristics. Biometric systems verify or identify a person by examining his physical features or behaviors. The first group of methods measures the physiological characteristics of a person (e.g. fingerprint, iris, ear shape and others). The latter group, i.e. based on behavioral characteristics, measures the behavior of a man (e.g. signature, keystroke dynamics, etc.).

Authentication systems are functioning mainly in verification mode [2]. This means that every user in order to be capable of being verified by the system shall successfully finish the enrolment (biometric characteristics acquisition), next transformed into feature vector and finally stored as biometric template in a database.
One shall assume that the whole population of users divides into genuine users and impostors. The impostors are making false attempts, i.e. try to be successfully verified by claiming to be someone else. The genuine users are making true attempts – they intentions are opposite to impostors' ones. During the verification the reference biometric template stored in database is compared with verification template acquired from the user. The result of the comparison is a confidence degree (e.g. expressed in percent) which is confronted with threshold value. If confidence degree is equal or greater than threshold value than the system accepts the attempt otherwise produces decision deny [11].

In order to properly present and analyze the anatomy of biometric authentication systems, a new easy-in-use methodology was needed. The only one that has appeared and has met the requirements was created by J. Ashbourn and named BANTAM – Biometric and Token Application Modeling Language [1].

As a fulfillment to presented theoretical aspects the model of biometric authentication system was created and visualized by means of notification symbols of BANTAM. The fig. 1 presents the model of biometric authentication system and depicts simple scenario depicted: the user interacts with biometric device which communicates with host application.

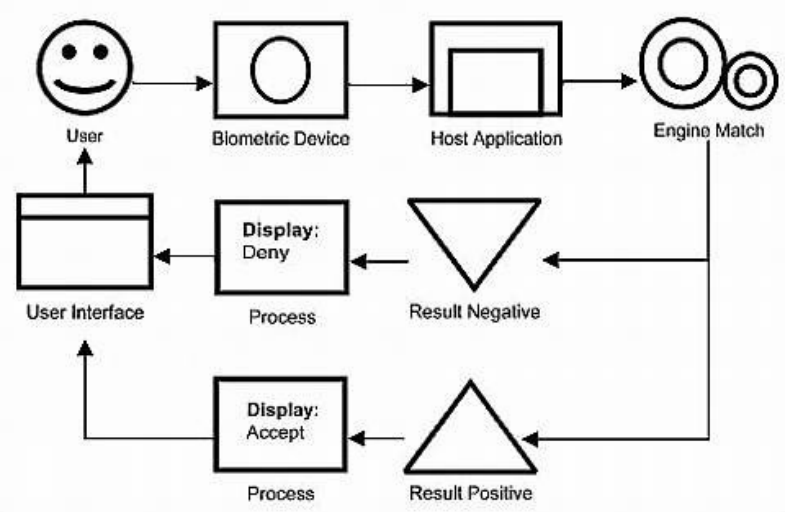

Fig. 1. Model of biometric authentication system¸

A matching process is undertaken which produces positive or negative result, each of which sends a message to the user interface.

In the next part of the article two methods of behavioral biometrics were presented.

3 Behavioral biometrics—keystroke

Keystroke dynamics, also known as typing rhythms, has a very long tradition in biometrics and is one of the most eagerly developed of all biometric technologies [15, 16]. It was observed in the end of the 19th century that telegraph operators could identify each other only by listening to the rhythm of their Morse code keying patterns. But the first intentional use of keystroke dynamics for person identification was in 1975 [12]. Since then it is generally approved that keystroke biometrics measure typing characteristics are unique to individual person and thus difficult to duplicate [13].

The authentication based on the schema login and password is the most common mechanism used to grand access to resources. Firstly it is low cost technology and besides it is familiarity to most of users. However this technology is often menaced because of week password and careless users. The answer for this problem is biometric technology – it is hard to imagine that biometric characteristics could be stolen, lost or forgotten (of course there are some difficult problems related we can't forget). Keystroke biometrics hold great promise to become standard method of user authentication. It's very inexpensive method without the need of any special hardware and has an advantage over other biometrics methods – users acceptance. Because using login and password to authenticate is obvious for most users and because of the fact, that keystroke dynamics may depend on these phrases, this technology could be almost completely transparent.

Analyzing keystroke dynamics is a process that analyzes the way users type by monitoring the keyboard inputs and then identifies users on their individual typing rhythm patterns. While the user is typing a string key down and up times are captured to achieve features: duration of the key and keystroke latency. Duration of the key is the time that a key remains pressed (time interval between pressing and releasing the key) and keystroke latency is the time between two keystrokes.

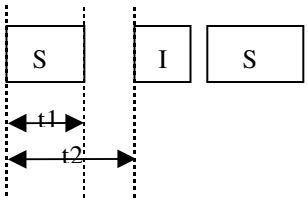

Fig. 2. A tree-key sequence "SIS" showing the measures: t1 = duration of first key (release time of first key – press time of first key) and t2 = latency between first and second key (press time of second key – press time of first key)

The main problem with measuring the time of pressing and releasing keys is timing accuracy. The results depends on the keyboard type, hardware, OS version, and computer configuration. Transfer of signal identifying a keypress from the keyboard to program can have large variability. The first aim to resolve the problem is to understand how keyboard, keyboard controller and software layer works in PCs.

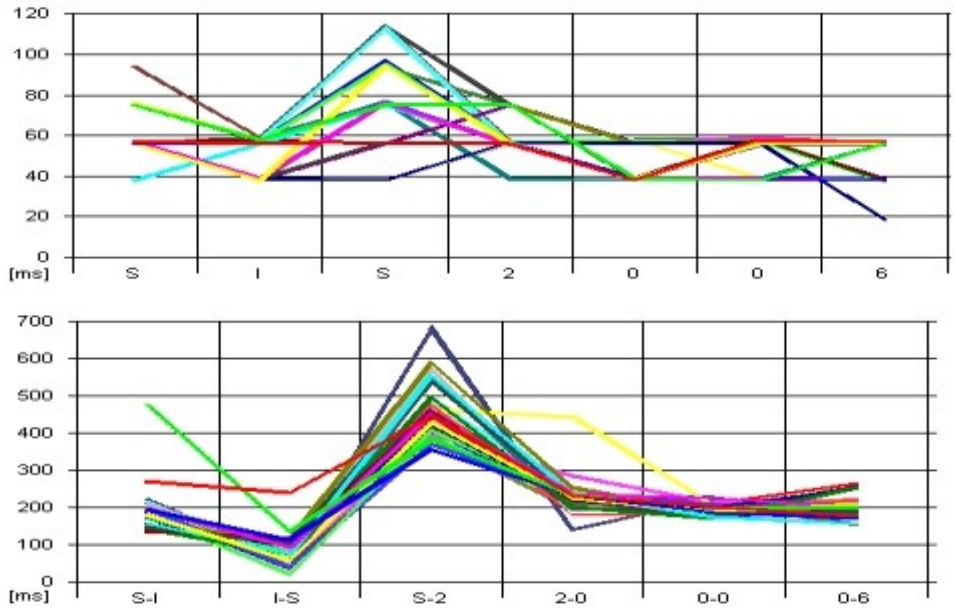

Fig. 3. Duration of the key and keystroke latency in string "SIS2006"

The keyboard is nowadays the primary input device for software on the PC system, so learning how it works is very important. Every keyboard has inside microcontroller chip that constantly scans a large matrix of keys to determine if any keys are down. To get rid of phenomenon known as keybounce, when contacts bounce off one another many times before coming to rest making a clean contact during a keypress, controller has a special scan algorithm, that employs delays while scanning keys. Therefore there is first place where some delay could be noticed. After capturing pressing or releasing key keyboard controller sent appropriate coded data to the host through serial communication channel according to IBM protocol. Computer also contains controller that is in charge of decoding all of the data received from keyboard controller and then they are processed by the keyboard's interrupt service routine. There are several methods how to receive pressed keys in operating system. In Microsoft Windows it can be achieve through: simple key events in application, hook mechanism, DirectX access or keyboard driver. According to established researches it can be assume, that delay of sending data, host keyboard controller and software layer is marginal in comparison with keybounce problem delay and transfer speed from keyboard to computer. We are now investigating how big influence has type of keyboard.

For experimentation purposes special Internet application was developed to collect users keystroke patterns and to demonstrate real-life working. ActiveX control was responsible for capturing data and measuring keystroke duration times and interval times at the accuracy of milliseconds. Forty seven users (men and women between 20 and 60 years old) participated in the experiment. They were asked to type login, password and fixed text "Politechnika", only this phrase was used to built users profiles. After the user has finished typing login, password an fixed string, statistics of the session where displayed including the individual durations and intervals for each keystroke together with the overall mean and variance.

Experiment was conducted using a statistical classifier based on distance and fixed common string "Politechnika" obtaining a 15% FRR (False Rejection Rate) and a 2% FAR (False Acceptance Rate).

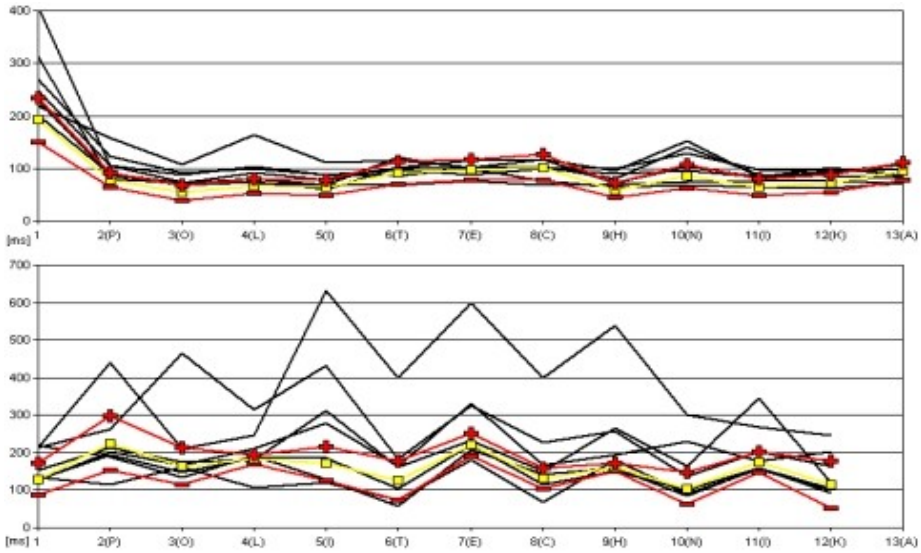

Fig. 4. Mean and variance of duration of the key and keystroke latency in fixed string "Politechnika" compared with other users mean.

4 Behavioral biometrics—eye movement

Eyes are one of the most important human organs. Therefore, it is not a surprise that using eyes to perform human identification in biometric methods has a long tradition including well established iris pattern recognition algorithms [3] or retina scanning. But these techniques measure only physiological parameters of eyes. Identifying people by the way they are *using* their eyes may be more interesting.

Eyes are the main 'interface' between environment and human brain and the system which deals with human vision is physiologically and neurologically complicated. To enable brain to acquire image in real time, the system which controls eye movements (termed *oculomotor system*) has to be very fast and accurate. It is built of six extra ocular muscles which act as three agonist/antagonist pairs concerned with horizontal, vertical and oblique rotations of eye [4]. Eyes are controlled directly by the brain with three cranial nerves originating from midbrain and pons. Therefore its movements are the fastest reactions for changing environment.

When individual looks at an object, the image of the object is projected on to the retina, which is composed of light-sensitive cells that convert light into signals which in turn can be transmitted to brain via the optic nerve. The density of this light-sensitive cells on retina is uneven, with denser clustering at the centre of the retina rather than at the periphery. Such clustering causes the acuity of vision to vary, with the most detailed vision available when the object of interest falls on the centre of the retina. This area is called yellow dot or fovea and covers about two degrees of visual angle. Outside this region visual acuity rapidly decreases. Eye movements are made to reorient the eye so that the object of interest falls upon the fovea and the highest level of detail can be extracted [5].

That is why it is possible to define a 'gaze point' – an exact point a person is looking at in a given moment of time. When eyes are looking at something for a period of time this state of the eye is called a fixation. During that time the image which is projected on the fovea is analyzed by the brain. The standard fixation lasts for about 200-300 ms, but of course it depends on the complexity of an image which is observed. After the fixation, eyes move rapidly to another gaze point – another fixation. This rapid movement is termed a saccade. Saccades differ in longitude, yet always are very fast.

Eye movements may give a lot of information about an individual. The way the gaze point is moving through the image is often the result of person's previous experience [6]. The experiment described in this paper used a 'jumping point' stimulation to observe person's reactions. It that kind of stimulation the screen is blank with

only one point 'jumping' through it. The task of examined persons is to follow the point with their eyes. There are nine different point placements defined on the screen, one in the middle and eight on the edges, creating 3 x 3 matrix. The point flashes in one placement in a given moment. The stimulation begins and ends with a point in the middle of the screen. During the stimulation, point's placement changes in specified intervals.

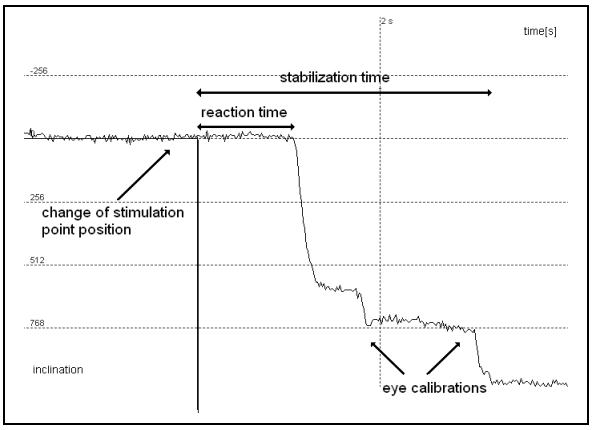

Fig. 5. Typical eye movement reaction for point jump in one axis. Reaction time is understood as the period of time between stimulation's change and eye reaction. Stabilization time is the time until fixation on a new gaze-point. Two calibration saccades may be observed

Data gathering process was described in details in [7]. The same test was preformed on 47 persons at the age ranging from 19 to 38, both males and females. There were overall 1151 experiments performed. Each experiment result was than transformed using several universal and subject specific transforms (like wavelets, eye distance etc.).

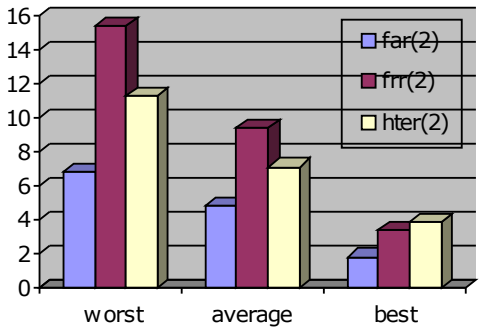

Fig. 6. Authorization errors for different persons

The described experiment produced a lot of data which was than analysed in EyeStat application [7]. The results of errors calculations were then averaged giving values presented in Table 1. Abbreviation FAR stands for False Acceptance Rate, abbreviation FRR stands for False Rejection Rate and Half Total Error Rate (HTER) is the average of both of them.

Table 1. Error rates in authorization test

	FAR(2)	FRR(2)	HTERR(2)
worst	6,83	15,38	11,25
average	**4,84**	**9,4**	**7,12**
best	1,82	3,44	3,88

5 Conclusions

In the article two chosen biometric methods were taken into in-depth analysis. The first method was based on keystroke dynamics and the second one was based on eye movement analysis.

The advantages of keystroke dynamics in user authentication are quite obvious. Assuming that the input device is the existing keyboard, this technology is only a cost of software and could be a standard in short time without many problems hinder other biometrics technologies. Differences in the physical characteristics of keyboards should be in special consideration in subsequent works. Measuring the time must be done as near keyboard device as possible to correctly track each pressed key and mark exactly time of press and release of key. Therefore keystroke dynamics could also come in the form of a built-in hardware in keyboards or motherboard, not only a software [14].

The idea of personal identification using eye movement characteristic seems to be valuable addition to other well known biometric techniques [8,9]. What makes it interesting is the easiness of combining it with, for instance, face or iris recognition. As all of those techniques need digital cameras to collect data, the system that uses the same recording devices to gather information about human face shape, eye iris pattern and eye movements characteristic may be developed. Of course there is a lot of work to be done to improve the methodology, but first experiments show the great potential of eye movements identification.

Further research work include implementations of described methods in real-life applications, including internet identification for purposes of e-learning and e-commerce solutions.

References

1. Ashbourn J.: *BANTAM*. Springer Verlag, London (2002).
2. Ashbourn J.: *Biometrics – advanced identity verification,* Springer Verlag (2000).
3. Daugman, J. G.: *High Confidence Visual Recognition of Persons by a Test of Statistical Independence,* IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. **15**, no. 11 (1993).
4. Hung G. K.: *Models of Oculomotor Control,* World Scientific Publishing Co. (2001)
5. Cowen, L., Ball, L. J., Delin, J.: *An eye-movement analysis of web-page usability,* Chapter in X. Faulkner, J. Finlay, & F. Détienne (Eds.): People and Computers XVI—Memorable Yet Invisible: Proceedings of HCI 2002. Springer-Verlag Ltd, London (2002).
6. Noton, D., Stark, L. W.: *Scanpaths in eye movements during pattern perception.* Science, 171 (1971).
7. Kasprowski P.: *Human Identification Using Eye Movements,* PhD Dissertation. Silesian University of Technology, Gliwice, Poland (2004).
8. Kasprowski P., Ober J.: *With the flick of an eye,* Biometrics Technology Today ISSN 0969-4765, Volume **12**, Issue 3, Elsevier Science (2004).
9. Kasprowski P., Ober J: *Eye Movement in Biometrics,* Proceedings of Biometric Authentication Workshop, European Conference on Computer Vision in Prague 2004, LNCS 3087, Springer-Verlag (2004).
10. Kapczyński A.: *About implementation of multiple biometrics authentication system,* Proceedings of 2nd International Conference on Information and communication technology security, Bielsko-Biala, Poland (2003).
11. Nanavanti S., Thieme M., Nanavati R.: *Biometrics - identity verification,* Wiley & Sons, Inc. (2002).
12. Spillane R.: *Keyboard Apparatus for Personal Identification,* IBM Technical Disclosure Bulletin, vol. **17**, no. 3346, 1975.
13. Leggett J.: *Dynamic Identity Verification via Keystroke Characteristics,* Int'l J. Man-Machine Studies, vol. **35**, no. 6, 1991, pp. 859–870.
14. Monrose F., Rubin A.D.: *Keystroke Dynamics as a Biometric for Authentication,* Future Generations Computing Systems, vol. **16**, no. 4, 2000, pp. 351–359.
15. Gaines R.: *Authentication by Keystroke Timing: Some Preliminary Results,* tech. report R-256-NSF, RAND, 1980.
16. Joyce R., Gupta G.: I*dentity Authentication Based on Keystroke Latencies,* Comm. ACM, vol. **33**, no. 2, 1990, pp. 168–176.